

**(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)**

**(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international**



**(43) Date de la publication internationale
30 juin 2005 (30.06.2005)**

PCT

**(10) Numéro de publication internationale
WO 2005/060160 A3**

(51) Classification internationale des brevets⁷ : H04L 12/24, 29/06

(71) Déposant (pour tous les États désignés sauf US) : FRANCE TELECOM [FR/FR]; 6 PLACE D'ALLERAY, F-75015 PARIS (FR).

(21) Numéro de la demande internationale : PCT/FR2004/003251

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : MORIN, Benjamin [FR/FR]; 22 RUE DES CROISIERS, F-14000 CAEN (FR). DEBAR, Hervé [FR/FR]; 7 RUE DES SEMAILLES, F-14111 LOUVIGNY (FR). TOMBINI, Elvis [FR/FR]; 1 RUE SOPHRONYME BEAUJOUR, F-14000 CAEN (FR).

(22) Date de dépôt international : 16 décembre 2004 (16.12.2004)

(74) Mandataires : JOLY, Jean-Jacques etc.; 158 RUE DE L'UNIVERSITE, F-75340 PARIS CEDEX 07 (FR).

(25) Langue de dépôt : français

(76) Langue de publication : français

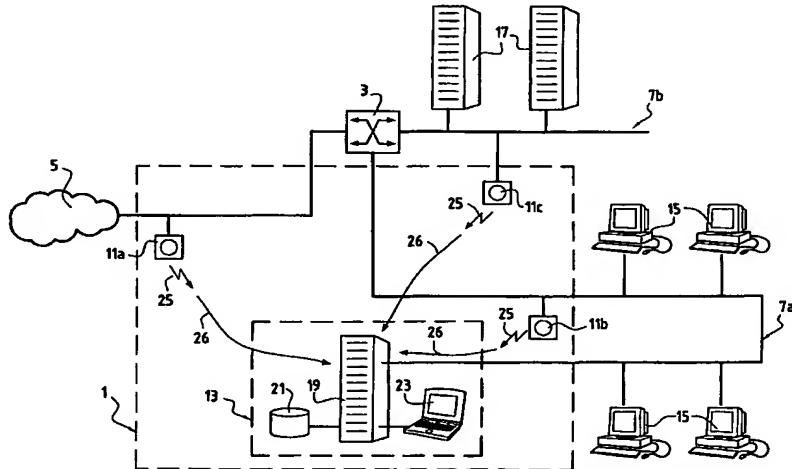
(30) Données relatives à la priorité : 0314782 17 décembre 2003 (17.12.2003) FR

(81) États désignés (sauf indication contraire, pour tout titre de protection nationale disponible) : AE, AG, AL, AM, AT,

[Suite sur la page suivante]

(54) Title: METHOD FOR AUTOMATICALLY CLASSIFYING A SET OF ALARMS EMITTED BY SENSORS FOR DETECTING INTRUSIONS OF A INFORMATION SECURITY SYSTEM

(54) Titre : PROCEDE DE CLASSIFICATION AUTOMATIQUE D'UN ENSEMBLE D'ALERTE ISSUES DE SONDES DE DETECTION D'INTRUSIONS D'UN SYSTEME DE SECURITE D'INFORMATION



(57) Abstract: The invention relates to a method for automatically classifying a set of alarms emitted by intrusion detecting sensors (11a, 11b, 11c) of an information security system (1) for producing synthetic alarms, wherein each alarm is defined by a plurality of qualitative attributes (a₁, a_n) allocated to a plurality of attribute ranges (A₁, A_n) consisting in organising the attributes allocated to each attribute range in to a multilevel hierarchical structure, constructing for each alarm emitted by intrusion detecting sensors (11a, 11b, 11c) a grating intrinsic to said alarm by generalising each alarm according to each attribute thereof and to all levels of the hierarchical structure, iteratively merging each intrinsic grating in a general grating, identifying, in a general grating, synthetic alarms by selecting the alarms which are simultaneously the most relevant and most general and in transmitting said synthetic alarms to the output unit (23) of an alarm managing system (13).

(57) Abrégé : L'invention concerne un procédé de classification automatique d'un ensemble d'alertes issues de sondes de détection d'intrusions (11a, 11b, 11c) d'un système de sécurité d'information (1) pour produire des alertes synthétiques, chaque alerte étant définie par une pluralité d'attributs qualitatifs

[Suite sur la page suivante]

WO 2005/060160 A3



AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

(88) Date de publication du rapport de recherche internationale:

15 septembre 2005

(84) États désignés (sauf indication contraire, pour tout titre de protection régionale disponible) : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.